



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/936,286

09/12/2001

Francois Cunchon

52003878

3967

88755 7590 08/13/2010

Bull HN Information Systems Inc.

Attn: Russell W. Guenthner

13430 N. Black Canyon Highway

Phoenix, AZ 85029-1348

EXAMINER

BATES, KEVIN T

ART UNIT

PAPER NUMBER

2456

MAIL DATE

DELIVERY MODE

08/13/2010

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 09/936,286	<b>Applicant(s)</b> CUNCHON ET AL.	
	<b>Examiner</b> KEVIN BATES	<b>Art Unit</b> 2456	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 02 July 2010.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 7, 10, 14, 20 and 22-25 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 7, 10, 14, 20 and 22-25 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)         | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)         | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____   | 6) <input type="checkbox"/> Other: _____                          |

***Response to Amendment***

This Office Action is in response to a communication made on July 2, 2010.

Claims 7, 10, 14, and 20 are currently amended.

Claims 24-25 are newly added.

Claims 7, 10, 14, 20, and 22-25 are pending in this application.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**Claims 7, 10, 20, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ilnicki (6751677) in view of Subramaniam (6081900).**

**Regarding claim 7**, Ilnicki teaches a method allowing a client application running on a client machine linked to a client network to establish communication with a server application hosted in a server machine linked to a server network in order to exchange messages with the server application, said messages passing between the client network and the server network through a network layer of a gateway machine (Figure 3), the method comprising:

A) receiving a request from the client application to establish communication at a first security level to a first port on the server machine (Col. 5, lines 21 -25);

Art Unit: 2456

B) creating a first port on the gateway machine (Col. 5, lines 4 – 13);

C) creating at least one first created process on the gateway machine (Col. 8, lines 46 – 57);

D) establishing a first connection from the client application to the first port on the gateway machine, the first connection connecting the client machine to the gateway machine for the exchange of messages at the first security level (Col. 5, lines 21 -25);

E) creating a second port in the gateway machine (Col. 8, lines 46 – 57);

F) establishing a second connection from the second port of the gateway machine to the first port of the server machine, the second connection to be used to exchange messages at a second security level which is reduced from the first security level (Col. 8, lines 46 – 57); and

G) rerouting to the second port of the gateway machine messages sent from the client network addressed to the first port of the server machine (Col. 8, lines 46 – 57);

H) routing, to the first port of the gateway machine, messages received by the gateway machine that are addressed to the client application on the client machine (Col. 8, lines 46 – 57).

Illnicki does not explicitly indicate the first created process on the gateway machine handling security processing at the first security level of encryption for said messages sent and said messages received on the first port of the gateway machine, thereby removing from the server machine, security processing at the second security of encryption level for these messages.

Subramaniam teaches a system which redirects requests to a target server to a gateway/border server which creates a secure encrypted connection from that gateway to the client and a second differently secured connection from the gateway to the target server (Col. 6, lines 40 – 45; Col. 7, lines 24 – 35; Col. 8, lines 13 – 19; Col. 9, lines 11 – 17).

It would have been obvious to one of ordinary skill in the art at the time the invention was made that Subramaniam's teaching can be incorporated into Ilnicki's system so that if the network is configured that the gateway gets places on the edge of a private network, a secure connection needs only to be maintained as far as the public network and the security session information does not need to be continued into the more secure private network.

**Regarding claim 10**, Ilnicki teaches a method according to claim 7, wherein said steps D, E, and F are executed automatically by the first created process of the gateway machine and wherein said first created process generates the second process that executes said steps G and H (Col. 5, lines 21 -25, wherein using different processes for different operations of the gateway is an obvious variation of any program run on a computer).

**Regarding claim 20**, Ilnicki teaches a method according to claim 7, further comprising deleting, by ordering the network layer of the gateway machine, messages sent from the client network to a port other than the first located in the server machine regardless of a security level of said message sent to the port (Col. 5, lines 60 – 65,

Art Unit: 2456

where if the port is unauthorized to be sent through the gateway, then the messages will not be allowed to pass through the gateway).

**Regarding claim 23**, Inicki teaches a method as claimed in claim 7, wherein the rerouting of the messages addressed to the first port of the server application is done in a way that is transparent to the client application (Col. 8, lines 46 – 57).

Regarding claim 24, Inicki in combination with Subramaniam teaches the method according to claim 7, wherein the second security level of encryption provides for exchange of messages which are unencrypted (See Subramaniam, Col. 9, lines 11-17).

**Claims 14 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Inicki in view of Subramaniam, and in further view of Rees (6981265).**

**Regarding claim 14**, Inicki teaches a method for allowing a client application to establish, in a client network, a first connection at a first security level with a first port of a server application hosted in a server machine linked to a server network, in order to send messages addressed to the server machine, said messages passing from the client network to the server network through a network layer of a gateway machine, the method comprising:

generating, in the gateway machine, a processing thread which establishes said first connection (Col. 5, lines 21 -25);

activating, in the gateway machine, a secure application proxy that performs security processing at the first security level and that reroutes the messages addressed

Art Unit: 2456

to the first port of the server application away from the first connection (Col. 5, lines 21 - 25); and,

establishing at a second security level, a second connection between a port of the server application and the gateway machine, said port being configured to receive at least one message at a second security level from the gateway machine via said second connection (Col. 8, lines 46 – 57), and

wherein said generating step is performed in response to detection of a request from the client application addressed to the first port of the server application to establish said first connection; and wherein said second connection is unknown to said client application (Col. 8, lines 46 – 57).

Ilnicki does not explicitly indicate that the gateway server establishes a connection with a second port of the server application, rather than a first port or that the second security level is lower than the first.

Rees teaches a system for relaying messages from an external network into an internal network through a gateway (Fig. 11) that includes a teaching that messages forwarded to port 1 of a port inside the network can be forwarded to a different port inside the network by the gateway (Col. 22, line 50 – Col. 23, line 20).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use Rees teaching of allowing the gateway redirect a communication from a first port to a second to allow communications external to the target server's network access ports which only internal user's can access.

Subramaniam teaches a system which redirects requests to a target server to a gateway/border server which creates a secure encrypted connection from that gateway to the client and a second differently secured connection from the gateway to the target server (Col. 6, lines 40 – 45; Col. 7, lines 24 – 35; Col. 8, lines 13 – 19; Col. 9, lines 11 – 17).

It would have been obvious to one of ordinary skill in the art at the time the invention was made that Subramaniam's teaching can be incorporated into Ilnicki's system so that if the network is configured that the gateway gets places on the edge of a private network, a secure connection needs only to be maintained as far as the public network and the security session information does not need to be continued into the more secure private network.

**Regarding claim 22**, Ilnicki teaches a method as claimed in claim 14, wherein the rerouting of the messages addressed to the first port of the server application is done in a way that is transparent to the client application (Col. 8, lines 46 – 57).

**Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ilnicki in view of Subramaniam, and in further view of Shimbo (6092191).**

Regarding claim 25, Ilnicki in combination of Subramaniam teaches the method according to claim 7, but does not explicitly indicate wherein the second security level of encryption is at a greater security level than a security level of no encryption.

Shimbo teaches a system with security gateways which intercept and redirect network traffic which includes the concept that each destination and each host can have



Art Unit: 2456

different levels of encryption designed to them, and the security gateway provides encryption services to allow those encryption services to be reached (Col. 33, lines 20 - Col. 34, line 2).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use Shimbo's teaching of encryption levels based on nodes in the network and using a gateway to alter the encryption level of information to allow client and servers in Ilnicki's system to operate at different encryption levels without having to negotiate those levels, including cases where the server receives information at a lower security level than the client is providing the information.

### ***Response to Arguments***

Applicant's arguments with respect to claims 7 and 14 have been considered but are moot in view of the new ground(s) of rejection.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KEVIN BATES whose telephone number is (571)272-3980. The examiner can normally be reached on M-F 8 am - 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on (571) 272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2456

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/KEVIN BATES/

Primary Examiner, Art Unit 2456